REMARKS

Claims 1-72 are pending. Claims 1-34, 36-37, 39, 41, 43-46, 49-50, and 52-72 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al. and Cavoukian "Building in Privacy" (Cavoukian). Claims 35 and 48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,233,618 to Herz. Claims 38 and 51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,233,618 to Shannon. Claim 40 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,011,858 to Stock et al. Claims 42 and 47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,119,096 to Mann et al.

The Examiner rejected claims 35, 38, 48, and 51 over Bianco in view of O'Flaherty and either Herz or Shannon. The Examiner identified both Herz and Shannon as having U.S. Patent No. 6,233,618. In the Office Action dated May 22, 2002, the Examiner identified Herz as U.S. Patent No. 6,029,195. The Office Action is interpreted as intending to use U.S. Patent No. 6,029,195 as the reference entitled Herz in rejecting claims 35 and 48. As this is the second Office Action to make this error, the Examiner is requested to ensure that future Office Actions accurately identify the references intended to be used in rejecting the claims.

Reconsideration is requested. No new matter is added. The rejections are traversed. Claims 1-72 remain in the case for consideration.

In ¶ 3 (page 2) of the Office Action dated December 30, 2004, the Examiner stated that "Applicant has not presented any arguments or assertions against the rejections". In ¶ 12 (page 20) of the same Office Action, the Examiner stated that "Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action". Finally, in rejecting the claims in the Office Action dated December 30, 2004, the Examiner has merely represented the arguments made in the Office Action dated July 19, 2004, and has presented no new arguments.

The Applicant would first point out that the assertions in ¶¶ 3 and 12 are mutually exclusive: if an Applicant does not present any arguments or assertions against the rejection, then the Applicant has not necessitated a new ground of rejection.

Second, both of these statements are incorrect. In response to the Office Action dated July 19, 2004, the Applicant made no amendments to the claims, but did present arguments as to why the claims are allowable over the references cited by the Examiner. A copy of the response to the Office Action dated July 19, 2004, is attached to hereto: the arguments can be found on pages 17-21 of this previous response. The Examiner is respectfully requested to consider this argument before issuing a new Office Action.

In addition, **the undersigned requests that the Examiner telephone the undersigned at (503) 222-3613 to schedule an interview at the Examiner's earliest convenience.**

For the foregoing reasons, reconsideration and allowance of claims 1-72 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
503-222-3613
Customer No. 20575

PATENT APPLICATION
MJM Do. No. 8514-25

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Ned HOFFMAN and Philip Dean LAPSLEY

Serial No. 09/398,914 Examiner: James A. REAGAN

Confirmation No. 1647

Filed: September 16, 1999 Group Art Unit: 3621

For: SYSTEM AND METHOD FOR PROCESSING TOKENLESS BIOMETRIC ELECTRONIC TRANSMISSIONS USING AN ELECTRONIC RULE MODULE CLEARINGHOUSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

Responsive to the Office Action, dated July 19, 2004, please amend the application as follows.

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims, which begins on page 2 of this paper.

REMARKS/ARGUMENTS begin on page 17 of this paper

IN THE CLAIMS

Please amend the claims to read as follows:

1. (Previously Presented) A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

a. a user registration step, wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

b. formation of a user-customizable rule module customized to the user in a rule module clearinghouse, wherein at least one pattern data of a user is associated with at least one execution command of the user;

c. a user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user;

d. a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission,

wherein a biometrically authorized electronic transmission is conducted without the user presenting smartcards or magnetic swipe cards.

2. (Original) The method of claim 1 wherein during the command execution step, the electronic rule module clearinghouse communicates with one or more third-party computers.

3. (Previously Presented) The method of claim 1 wherein said execution commands are comprised of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules.

4. (Previously Presented) The method of claim 1 wherein pattern data comprises one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing

patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

5. (Previously Presented) The method of claim 1, wherein pattern data for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

6. (Previously Presented) The method of claim 1, wherein an execution command for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

7. (Original) The method of claim 1 further comprising a user re-registration check step, wherein the user's registration biometric sample is compared against previously registered biometric samples wherein if a match occurs, the computer system is alerted to the fact that the user has attempted to re-register with the electronic identicator.

8. (Previously Presented) The method of claim 1 wherein the biometric sample comprises one or more of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

9. (Original) The method of claim 1 wherein during the identification step, the user provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

10. (Original) The method of claim 9 further comprising a biometric theft resolution step, wherein a user's personal identification code is changed when the user's biometric sample is determined to have been fraudulently duplicated.

11. (Original) The method of claim 1, wherein execution of an execution command authorizes the user to access stored electronic data.

12. (Original) The method of claim 11 wherein accessing stored electronic data results in activation of an Internet-connected device.

13. (Original) The method of claim 1 wherein executing an execution command processes electronic data to provide the user with a user requested electronic transmission.

14. (Previously Presented) The method of claim 13, wherein said processing comprises invoking one or more of the following: a user's digital certificate, a user's identity scrambler, a user's interactive electronic consumer loyalty or consumer rewards program, a user's interactive electronic advertising, a user's interactive instant messaging program, a user's email authentication, and an automated electronic intelligent agent for electronic data search and retrieval that is customized to the user's requests.

15. (Original) The method of claim 1 wherein executing an execution command presents electronic data that is customized to the user's requested electronic transmission.

16. (Original) The method of claim 1 further comprising a user log-in repeat step, wherein during an electronic transmission the user is periodically required by the electronic identicator to present the user's bid biometric sample or at least one of the user's pattern data.

17. (Previously Presented) The method of claim 1 further comprising a communications step wherein one or more of the following is used: the Internet, an intranet, an extranet, a local area network, and a wide area network.

18. (Previously Presented) The method of claim 1 further comprising a third-party registration step, wherein a third-party registers identification data with the electronic identicator, the identification data comprising one or more of the following: a biometric, a digital certificate, an Internet protocol address, and a biometric input apparatus hardware identification code.

19. (Original) The method of claim 18 further comprising a third-party identification step, wherein a third-party providing the user with electronic transmissions is identified by the electronic identicator by comparing the third-party's bid identification data with the third-party's registered identification data.

20. (Previously Presented) A computer system device for tokenless biometric processing of electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, comprising:

a. a biometric input apparatus, for providing a bid or registration biometric sample of a user to the electronic identicator, wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

b. an electronic rule module clearinghouse, having at least one user-customizable rule module further comprising at least one pattern data of the user associated with at least one execution command of the user, for executing at least one electronic transmission;

c. an electronic identicator, for comparing the bid biometric sample with registered biometric samples of users;

d. a command execution module, for invoking at least one previously designated execution command in the electronic rule module clearinghouse to execute an electronic transmission;

wherein no smartcards or magnetic swipe cards are presented by the user to conduct the electronic transmission.

21. (Original) The device of claim 20 wherein the command execution module communicates with one or more third-party computers.

22. (Previously Presented) The device of claim 20 wherein pattern data comprises one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant

messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

23. (Previously Presented) The device of claim 20, wherein pattern data for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

24. (Previously Presented) The device of claim 20, wherein an execution command for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

25. (Previously Presented) A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

a. a primary and subordinated user registration step, wherein a primary and subordinated user each register with an electronic identicator at least one registration biometric sample taken directly from the person of the primary and subordinated user, respectively;

b. formation of a rule module customized to the primary and subordinated user in a rule module clearinghouse, wherein at least one pattern data of the primary and subordinated user is associated with at least one execution command of the primary and subordinated user, the rule module customized to the primary user is customizable by the primary user and the rule module customized to the subordinated user is customizable by the subordinated user;

c. a subordinated user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the subordinated user with at least one previously registered biometric sample for producing either a successful or failed identification of the subordinated user;

d. a subordination step wherein upon successful identification of the subordinated user, the pattern data of the subordinated user is searched to determine if any of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules; and

e. a command execution step, wherein upon the successful identification of the subordinated user and the determination that at least one of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules, at least one previously designated execution command of the primary user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the primary and subordinated user presenting smartcards or magnetic swipe cards.

26. (Previously Presented) The method of claim 3 wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

27. (Previously Presented) The method of claim 26 wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

28. (Previously Presented) The method of claim 26 wherein accessing membership benefits further comprises one or more of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to access an Internet web site; and validating a user's eligibility to enter a real-time internet chat room with other people on-line.

29. (Previously Presented) The method of claim 26 wherein accessing event admittance further comprises one or more of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres; and validating a user's eligibility to board a vehicle of travel.

30. (Previously Presented) The method of claim 11 wherein accessing stored electronic data comprises accessing one or more of the following: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content;

on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content; and server-based computer software programs and hardware drivers.

31. (Previously Presented) The method of claim 1 wherein at least one rule module further comprises one or more of the following: at least one pattern data associated with at least two execution commands; and at least one execution command associated with at least two pattern data.

32. (Previously Presented) The method of claim 12 wherein activation of an internet-connected device further comprises activating one or more of the following devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine; and a digital audio player.

33. (Previously Presented) The method of claim 14 wherein the automated intelligent agent for electronic data search and retrieval further comprises conducting periodic, user-customized on-line retrievals for one or more of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements; and faxes.

34. (Previously Presented) The method of claim 29 wherein the vehicle of travel further comprises one or more of the following: an airplane; a train; a boat; and a bus.

35. (Previously Presented) The method of claim 14 wherein the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future.

36. (Previously Presented) The method of claim 14 wherein invoking a user's digital certificate with an electronic transmission to verify the authenticity of the

sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

37. (Previously Presented) The method of claim 13 wherein the processing of electronic transmissions further comprises execution commands which filter the access and presentation of data when the user is subordinated user.

38. (Previously Presented) The method of claim 37 wherein the filter governs subordinated user access to one or more of the following: Internet web sites with adult content; Internet sites with violent content; on-line session length; and educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user.

39. (Previously Presented) The device of claim 20 wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

40. (Previously Presented) The device of claim 39 wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

41. (Previously Presented) The device of claim 39 wherein accessing membership benefits further comprises one or more of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to access an Internet web site; and validating a user's eligibility to enter a real-time internet chat room with other people on-line.

42. (Previously Presented) The device of claim 39 wherein accessing event admittance further comprises one or more of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-

rated film being shown in theatres; and validating a user's eligibility to board a vehicle of travel.

43. (Previously Presented) The device of claim 20 wherein execution commands further comprise accessing one or more of the following stored electronic data: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content; and server-based computer software programs and hardware drivers.

44. (Previously Presented) The device of claim 20 wherein at least one rule module further comprises one or more of the following: at least one pattern data associated with at least two execution commands, and at least one execution command associated with at least two pattern data.

45. (Previously Presented) The device of claim 20 wherein execution commands further comprise activation of one or more of the following Internet-connected devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine; and a digital audio player.

46. (Previously Presented) The device of claim 20 wherein execution commands further comprise an automated intelligent agent for electronic data search and retrieval which conducts periodic, user-customized on-line retrievals for one or more of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements; and faxes.

47. (Previously Presented) The device of claim 42 wherein the vehicle of travel further comprises one or more of the following: an airplane; a train; a boat; and a bus.

48. (Previously Presented) The device of claim 46 wherein the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand

and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future.

49. (Previously Presented) The device of claim 20 wherein execution commands further comprise invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

50. (Previously Presented) The device of claim 20 wherein execution commands further comprise the processing of electronic transmissions which filter the access and presentation of data when the user is subordinated user.

51. (Previously Presented) The device of claim 50 wherein the filter governs subordinated user access to one or more of the following: Internet web sites with adult content; Internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user.

52. (Previously Presented) The method of claim 4 wherein said execution commands are comprised of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules.

53. (Previously Presented) The method of claim 53 wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

54. (Previously Presented) A biometric method implemented in a computer system for processing electronic transmissions, comprising:

registering at least one registration biometric sample taken directly from a user;

forming a user-customizable rule module customized to the user in a rule module clearinghouse, the rule module associating at least one pattern data of the user with at least one execution command of the user;

comparing a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed match; and

invoking the rule module of the user upon a successful match to execute at least one electronic transmission.

55. (Previously Presented) The method of claim 54, wherein the electronic transmission is executed without the user presenting smartcards or magnetic swipe cards.

56. (Previously Presented) The method of claim 54, wherein registering at least one registration biometric sample includes:

registering a plurality of biometric samples from a plurality of users; and

basketing a subset of the plurality of samples to facilitate the comparison with the bid biometric sample.

57. (Previously Presented) The method of claim 54, wherein comparing a bid biometric sample includes comparing the bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user.

58. (Previously Presented) The method of claim 54, wherein:

the execution command includes of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules; and

the execution command for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

59. (Previously Presented) The method of claim 54, wherein the execution command includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

60. (Previously Presented) The method of claim 59, wherein:

the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and

the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

61. (Previously Presented) The method of claim 54, wherein:

the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and

the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

62. (Previously Presented) The method of claim 54, wherein:

the pattern data includes demographic information of the user; and the execution command includes accessing stored electronic data to determine eligibility to purchase restricted products or to access data or services.

63. (Currently Amended) A biometric method implemented in a computer system for processing electronic transmissions, comprising:

registering at least one primary registration biometric sample taken directly from a primary user;

registering at least one secondary registration biometric sample taken directly from a secondary user;

forming a primary user-customizable rule module customized to the primary user in a rule module clearinghouse, the primary rule module associating at least one primary pattern data of the primary user with at least one primary execution command of the primary user;

forming a secondary user-customizable rule module customized to the secondary user in the rule module clearinghouse, the secondary rule module associating at least one secondary pattern data of the user with at least one secondary execution command of the secondary user;

subordinating the secondary rule module to the primary rule module;

comparing a bid biometric sample taken directly from the person of the secondary user with at least one previously registered biometric sample for producing either a successful or failed match;

determining that the secondary rule module is subordinated to the primary rule module; and

invoking the primary rule module of the primary user upon a successful match to execute at least one electronic transmission.

64. (Previously Presented) A computer system device for biometric processing of electronic transmissions, comprising:

a biometric input apparatus, for providing a bid or registration biometric sample of a user;

an electronic rule module clearinghouse, having at least one user-customizable rule module including at least one pattern data of the user associated with at least one execution command of the user;

an electronic identicator, to compare at least one registration biometric sample stored in the electronic identicator with a bid biometric sample to produce either a successful or failed match; and

a command execution module, to invoke at least one execution command in the electronic rule module clearinghouse to execute an electronic transmission.

65. (Previously Presented) The computer system of claim 64, wherein the electronic transmission is executed without the user presenting smartcards or magnetic swipe cards.

66. (Previously Presented) The computer system of claim 64, further comprising:

storage for a plurality of registration biometric samples from a plurality of users; and

means for basketing a subset of the plurality of samples in the storage to facilitate the comparison with the bid biometric sample.

67. (Previously Presented) The computer system of claim 64, wherein the electronic identicator is operative to compare at least one registration biometric sample stored in the electronic identicator with the bid biometric sample to produce either a successful or failed identification of the user.

68. (Previously Presented) The computer system of claim 64, wherein:

the execution command includes of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules; and

the execution command for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

69. (Previously Presented) The computer system of claim 64, wherein:

the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and

the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

70. (Previously Presented) The computer system of claim 69, wherein the execution command for accessing stored electronic data includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

71. (Previously Presented) The computer system of claim 64, wherein the execution command for accessing stored electronic data includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

72. (Previously Presented) The computer system of claim 64, wherein:

the pattern data includes demographic information of the user; and

the execution command includes accessing stored electronic data to determine eligibility to purchase restricted products or to access data or services.

REMARKS

Claims 1-34, 36-37, 39, 41, 43-46, 49-50, and 52-72 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al. and Cavoukian "Building in Privacy" (Cavoukian). Claims 35 and 48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,233,618 to Herz. Claims 38 and 51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,233,618 to Shannon. Claim 40 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,011,858 to Stock et al. Claims 42 and 47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,119,096 to Mann et al.

The Examiner rejected claims 35, 38, 48, and 51 over Bianco in view of O'Flaherty and either Herz or Shannon. The Examiner identified both Herz and Shannon as having U.S. Patent No. 6,233,618. In the Office Action dated May 22, 2002, the Examiner identified Herz as U.S. Patent No. 6,029,195. The Office Action is interpreted as intending to use U.S. Patent No. 6,029,195 as the reference entitled Herz in rejecting claims 35 and 48.

Reconsideration is requested. No new matter is added. The rejections are traversed. Claims 1-72 remain in the case for consideration.

REJECTIONS UNDER 35 U.S.C. § 103(a)

Referring to claim 1, the invention is directed toward a method for processing electronic transactions. A user registers with an electronic identicator a registration biometric sample. The user formulates a rule module in a clearinghouse. The rule includes at least one pattern data and at least one execution command. The user is then identified by comparing a bid biometric sample against the biometric samples registered in the electronic identicator. Assuming the user is identified, a rule module of the user is invoked, to execute at least one electronic transmission.

Referring to claim 20, the invention is a system for processing electronic transactions. A biometric input apparatus is used, for providing a registration biometric sample to an electronic identicator during registration, and for providing a bid biometric sample to the electronic identicator when the user wants to execute an electronic transmission. A clearinghouse stores rule modules, combining pattern data with execution commands. An execution module invokes an execution command from a rule module, responsive to the electronic identicator indicating whether the user is successfully identified.

Referring to claim 25, the invention is a method for processing electronic transactions. Two users, a primary and a subordinate, each register biometric samples with an electronic identicator. The users also formulate rule modules, associating pattern data with execution commands. The subordinated user is then identified by the electronic identicator. Assuming the subordinated user is successfully identified, the subordinated user's rule modules are checked to see if they are subordinated to any of the primary user's rule modules. Assuming that one of the subordinated user's rule modules are subordinated to one of the primary user's rule modules, the primary user's rule modules are invoked, thereby executing an electronic transmission.

Referring to claim 54, the invention is a method for processing electronic transactions. A biometric sample is registered. A user-customizable rule module is formed, including at least one pattern data of the user and at least one execution command of the user. A bid biometric sample is compared with the registered biometric sample. If the comparison indicates a successful match, the rule module is invoked.

Referring to claim 63, the invention is directed toward a method for processing electronic transactions. A primary user registers a primary registration biometric sample. A secondary user registers a secondary registration biometric sample. A primary user-customizable rule module, customized to the primary user, is formed, including at least one primary pattern data of the user and at least one primary execution command of the primary user. A secondary user-customizable rule module, customized to the secondary user, is formed, including at least one secondary pattern data of the user and at least one secondary execution command of the secondary user. The secondary rule module is subordinated to the primary rule module. A bid biometric sample taken from the secondary user is compared with at least one previously registered biometric sample. The secondary rule module is determined to be subordinated to the primary rule module. Upon a successful match, the primary rule module is invoked.

Referring to claim 64, the invention is directed toward a device for processing electronic transactions. A biometric input apparatus can provide a bid or registration biometric sample of a user. An electronic rule module clearinghouse can have at least one user-customizable rule module, including at least one pattern data of the user and at least one execution command of the user. An electronic identicator can compare a registration biometric sample with a bid biometric sample. A command execution module can execute at least one execution command.

In all of the foregoing claims, the rule modules is invoked *after* identification of the user.

In contrast to all of the foregoing claims, Bianco teaches a system for authenticating users and granting conditional access to resources. In Bianco, the user provides a user ID. The biometric group to which the user belongs is determined: the biometric policy of the biometric group controlling the authentication of the user. The user's registered biometric sample, associated with the user ID, is also determined. The user's biometric sample is compared with the registered sample. If the samples match according to the biometric policy, then the resources associated with the biometric group may be accessed by the user.

As argued in the Response to the Office Action dated May 22, 2002, there are several differences between the invention and the cited prior art. In the Interview Summary dated August 27, 2003, the Examiner indicated that some of these points were discussed. These points were, in the order mentioned by the Examiner, that identification as described in the claims "is distinct from the authorization and validation techniques of Bianco"; that the rule modules of the claims are user-customizable, whereas Bianco's rule modules are not user-customizable; and that the rules in Bianco are applied pre-authentication, whereas the rule modules of the claims are applied post-identification. In other words, the Examiner agreed with the Applicant that there were at least three points on which the claims could be distinguished over Bianco.

In rejecting the claims in the Office Action dated July 19, 2004, the Examiner has combined Bianco with two additional references: the published patent application of O'Flaherty and the Cavoukian article. The Examiner cites to O'Flaherty only to find support in the prior art for users to be able to customize data in a database. The Examiner's stated reason for including Cavoukian is that Cavoukian teaches biometric identification and authentication.

With reference to Cavoukian, the Applicant believes the articles is self-contradictory. The Applicant acknowledges that Cavoukian describes "biometrics [as] permit[ting] authentication without identification of the user". But the Applicant is lost in understanding how biometrics could be used in this way. Biometrics are inherently unique to the individual. Thus, a biometric taken from person A will, by definition, be different from a similar biometric taken from person B. Thus, if person A provides the biometric, the only person the biometric should match in the database is person A, meaning that person A has been identified.

The only reasonable interpretation of Cavoukian is that the database storing the "bioscrypts" does not associate the "bioscrypt" with a person's name. But this does not mean that the person is not identified; it only means that the person's name is not directly associated with the "bioscrypt". Clearly, it would take only a trivial modification of the database to associate the person's name with the "bioscrypt".

Cavoukian goes on to recite that "the bioscrypt bears no physical resemblance to the user's actual fingerprint. [The] system does not retain any record, image or template of the individual's actual fingerprint. Therefore, a copy of the fingerprint is never kept on file." But this does not mean that the individual is not uniquely identified in the database when a match is found. This comment only means that the process is not reversible: given a "bioscrpyt", the original fingerprint cannot be derived.

To use Cavoukian's example, she describes the use of biometrics to obtain welfare benefits "anonymously". But the "anonymity" to which Cavoukian refers is not a lack of identification; it is simply denying the name of recipient to the person offering the services. Because the government would not want welfare benefits to be provided to persons not entitled, somewhere there would be a database of biometrics of each legitimate welfare recipient. Each biometric in that database matches a biometric of a person. By not including the name of the welfare recipient, the services provider is not told the *name* of the welfare recipient. But because the government limits welfare benefits, the government would want to know what benefits have been received by which recipients. Thus, the recipient is identified to the government; he is anonymous only to the services provider.

To further elaborate, consider the following. If a person enters a store and says that his name is "John Smith", that name does not uniquely identify him. After all, he could be the John Smith from Los Angeles, CA, or the John Smith from Miami, FL. A name does not necessarily identify; we openly state that names are unique, but when pressed will admit that names are not necessarily unique. That is why, for example, drivers' licenses have unique numbers as issued by the state: the combination of the issuing state and the license number uniquely identify the individual, in a way a name never could.

Thus Cavoukian, despite the language of her article, does not in fact accomplish what she says is her goal. And this makes sense: if an individual cannot be identified, he cannot be personally held responsible for his actions. Such anonymity is unacceptable in most endeavors in life. Thus, Cavoukian's "anonymity" is not is not true anonymity, whereby a person is never uniquely identified; her "anonymity" is only from the people to whom the identity is not relevant. Against parties that want to know the person's identity, there is no anonymity.

Finally, Cavoukian only explains the benefits of her pseudo-anonymity. She does not explain how it might be implemented. Thus, Cavoukian can at best be said to explain why one might want to implement her scheme; the article fails to enable a system that provides pseudo-anonymity. Because Cavoukian is not an enabling description, its teaching is insufficient to render the claims obvious.

The Applicant also believes the Examiner has failed to make a prima facie argument that the claims are obvious, because the Examiner has failed to present arguments that the prior art teaches biometric identification or applying the rule modules after identification. All arguments made previously are hereby resubmitted.

As said in the Response to the Office Action of November 4, 2003, it makes no sense to provide *users* the ability to modify the biometric policies in Bianco. As stated at column 2, lines 61-63, "the biometric policies determine the way or method in which a user is to be authenticated by the system." In other words, the biometric policies specify how the user gains access to resources on the system. If users could modify the biometric policies, they could weaken the security associated with resource access, even to the point of not requiring any security at all. Clearly, a system that allows the user to modify the security associated with accessing a resource is no more secure than a system without any access control at all. Since security and access control are important to Bianco, it would make the Bianco system inoperative for its intended purpose, and therefore would not be obvious to give users the ability to change the security of the system, as would happen if Bianco and O'Flaherty were combined as suggested by the Examiner.

Even if the Examiner intended to analogize between the biometric groups (instead of the biometric policies) of Bianco with rule modules in the claims, the analogy still fails. As argued in the Response to the Office Action dated May 22, 2002, the biometric groups are used to determine which biometric policies to apply in authenticating the user, which means that the biometric groups are used *before* the user is authenticated, and not after the user is identified as claimed.

For the foregoing reasons, reconsideration and allowance of claims 1-72 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
503-222-3613
Customer No. 20575

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO:

□ COMMISSIONER OF PATENTS AND TRADEMARKS WASHINGTON D.C. 20231

☒ MAIL STOP Amendment
COMMISSIONER FOR PATENTS
BOX 1450
ALEXANDRIA, VA 22313-1450

□ BOX ________
COMMISSIONER FOR TRADEMARKS 2900 CRYSTAL DRIVE ARLINGTON, VA 22202-3513

ON: 23 Sept 2004